

Adding a RBAC Rights Profile to Solaris 11

Solaris 11 (Build 173) no longer contains a Primary Administrators rights profile. The Primary Administrator rights profile is a profile that is the equivalent of the root account. A user that holds the Primary Administrator right profile can become root with out assuming the Role of root by simply executing a profile shell. For example:

```
tim@sol11-server:~$ id
uid=60004(tim) gid=10(staff)
tim@sol11-server:~$ pfbash
root@sol11-server:~# id
uid=0(root) gid=0(root)
```

While this is a easy way to transition to root privileges it is not secure. This method reduces the security of the root account to the security of the password of the non-root user assigned the Primary Administrators rights profile. This may be in violation of organizational security policies and should be used with great care.

To add the rights profile to Solaris 11 you need to edit the appropriate files under the `/etc/security` directory. In Solaris 11 the traditional `prof_attr` and `exec_attr` files are now links to the `local-entries` files in `/etc/security/prof_attr.d` and the `/etc/exec_attr.d` directories respectively.

```
root@sol11-server:/etc/security# ls
audit_class      auth_attr.d      exec_attr        lib              prof_attr.d
audit_event      crypt.conf       exec_attr.d     policy.conf      tcsd.conf
audit_warn       dev              extra_privs      priv_names
auth_attr        device_policy   kmfpolicy.xml   prof_attr
```

```
root@sol11-server:/etc/security# cd prof_attr.d

root@sol11-server:/etc/security/prof_attr.d# ls -l local-entries
lrwxrwxrwx  1 root      root              12 Sep 16 16:15 local-entries -> ../prof_attr

root@sol11-server:/etc/security/prof_attr.d# ls
core-os                ntp
cups                   service-network-ftp
desktop-login          system-library-dbus
developer-dtrace-toolkit  system%2Fmanagement%2Fservice-tag
library-audio-gstreamer  trousers
local-entries           xserver-common

root@sol11-server:/etc/security/prof_attr.d# cat local-entries

#
# The system provided entries are stored in different files
# under "/etc/security/prof_attr.d".  They should not be
# copied to this file.
#
# Only local changes should be stored in this file.
# This line should be kept in this file or it will be overwritten.
#
```

To add the Primary Administrator right profile modify the `/etc/security/prof_attr.d/local-entries` file to add the following line:

```
Primary Administrator:::Prom all Administrative tasks:auths=solaris.*,solaris.grant
```

```
root@sol11-server:/etc/security/prof_attr.d# cat local-entries
```

```
#  
# The system provided entries are stored in different files  
# under "/etc/security/prof_attr.d". They should not be  
# copied to this file.  
#  
# Only local changes should be stored in this file.  
# This line should be kept in this file or it will be overwritten.  
#
```

```
Primary Administrator:::Prom all Administrative tasks:auths=solaris.*,solaris.grant
```

After saving the file add the following line to the `/etc/security/exec_attr.d/local-entries` files and save the file:

```
Primary Administrator:suser:cmd:::*:uid=0;gid=0
```

```
root@sol11-server:/etc/security/exec_attr.d# cat local-entries
```

```
#  
# The system provided entries are stored in different files  
# under "/etc/security/exec_attr.d". They should not be  
# copied to this file.  
#  
# Only local changes should be stored in this file.  
# This line should be kept in this file or it will be overwritten.  
#
```

```
Primary Administrator:suser:cmd:::*:uid=0;gid=0
```

You can now add the rights profile to the user:

```
root@sol11-server:/# usermod -P "Primary Administrator" tim
```

Again, because of security considerations this is not recommended for production servers. I use this on VirtualBox sandbox Solaris 11 servers only.